PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : G06F 17/30	A1	(11) International Publication Number: WO 00/26823
		(43) International Publication Date: 11 May 2000 (11.05.00)

(21) International Application Number: PCT/US99/26090

(22) International Filing Date: 4 November 1999 (04.11.99)

(30) Priority Data:

09/185,528	4 November 1998 (04.11.98)	US
09/385,575	30 August 1999 (30.08.99)	US

(71) Applicant *(for all designated States except US)*: GARFINKLE LIMITED PARTNERSHIP II [US/US]; 133 East 62nd Street, New York, NY 10021 (US).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: GARFINKLE, Norton [US/US]; 133 East 62nd Street, New York, NY 10021 (US).

(74) Agent: MARHOEFER, Laurence, J.; Lane, Aitken & McCann, Suite 901, 2600 Virginia Avenue, N.W., Washington, DC 20037 (US).

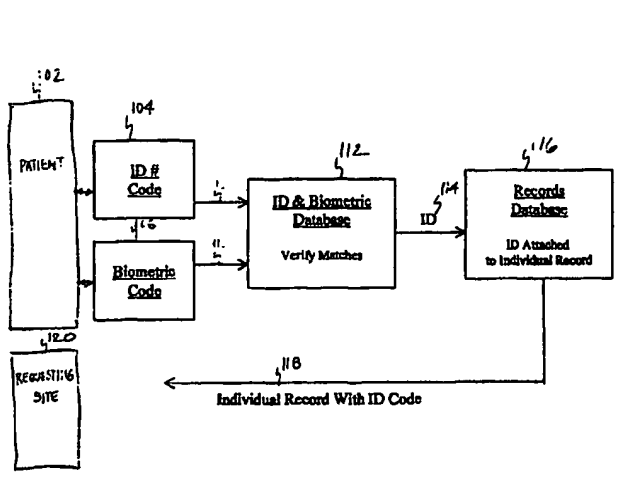
(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published

With international search report.

Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: A SYSTEM FOR PROTECTION OF UNAUTHORIZED ENTRY INTO ACCESSING RECORDS IN A RECORD DATABASE



(57) Abstract

A method for maintaining an individual's records in a record database (116). For example, a national medical record database protected by a digital code (104) generated by a physical characteristic of the person such as an encoded finger print, voice print, signature scan, or retinal scan that can be attached to a person's protected record (110) in the database in addition to a person's assigned ID code (104) such as a Social Security Number (116). Access via the ID can be selected in accordance with pre-established instructions mandated by an individual (118). For example, some individuals (102) will be more interested in medical personnel having ready access to their record and can specify instructions consistent with this concern. Some individuals (102) may be concerned with the privacy of certain parts of their medical history while others may not be concerned and can specify instructions consistent with this concern.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

SYSTEM FOR PROTECTING FROM UNAUTHORIZED ENTRY INTO AND/OR ACCESS TO RECORDS IN A RECORD DATABASE

Field of the Invention

The present invention relates to an improved system for protecting from unauthorized access to and/or entry into records of individuals in a database, and more particularly to a system for protecting medical records in a national medical record database.

Background of the Invention

As a person moves from birth to death, health care providers make records of his or her state of health and the medical intervention provided. A person's entire record includes record fragments recorded at different times, and usually recorded and stored at different physical locations. These record fragments include records stored on paper and film and more recently digital data records.

The doctor's office, hospital, HMO, or other medical entity that prepares the record usually stores the record at a physical location it selects, using its own addressing and security systems to access and protect the record. The entity that prepares the record usually considers the record to be its property, rather than the property of the patient. The present state of medical records provides relatively good physical security for the records. Digital records stored in a database are typically accessible only over a secure local network. In addition, there is today no practical way to access a complete medical history of a person when different record fragments are stored by different health care entities. Transfer of data

between health care entities is slow at best and not practical at all in many instances due to incompatibility of the databases.

Relatively recent technologies, such as the Internet and large database managers, have made it practical to have a national medical record database where a health care provider could easily and immediately access a patient's medical records prepared by any entity at any time. Access can be over a public network such as the Internet using web browser technology. The national medical record database could reside in one or more physical databases. The data could also reside in the databases of the health care entities that prepared them with hyper-links to a patient's record in each database so that the entire record could be assembled via the Internet using web browser technology. A combination of physical and virtual databases could be used. In any case, each person will have a medical identification (ID) for use in addressing the national medical record database when storing data in it or retrieving data from it. This ID could be preexisting personal numbers, special PIN numbers selected in secret, or a specific number issued by the manager of the national record database. While the advantages of a national medical database in providing improved care are clear, such a database raises data security concerns. Today, most medical records are not accessible over a public network. With a national medical record database, most medical records would be accessible. Today, an authorized or unauthorized person must know not only whose record he or she wants, but also where the record is kept and how to access records from that database. Tomorrow without increased security the unauthorized person may need to know only a person's medical ID and how to access the national medical database.

It is thus desirable that a more secure way of controlling access to a record such as, e.g., a medical record, be provided.

Summary of the Invention

A feature of the present invention is a system that protects a record of an individual in a central database from access by unauthorized parties. More particularly, the present invention can protect against unauthorized access of a record in a central database accessible via a public network such as, e.g., the Internet.

The present invention contemplates records in a central database (e.g., a national medical record database or a central financial database) protected by personal identification codes. Personal identification codes can include a person's assigned ID code. Examples of a person's assigned ID code include, e.g., a Universal Health Identification number, a Social Security number, or other alphanumeric string. Personal identification codes can also include biometrics, such as, e.g., one or more digital codes generated by one or more biometric physical characteristics of a person. Biometric physical characteristics of a person can include, e.g., an encoded finger print, a voice print, a signature print or a retinal scan.

These personal identification codes (assigned ID codes and biometrics) can be used to control access to a central database. For example, the personal identification codes can be used to grant access to certain approved individuals to the central database, and to identify and grant access to a particular record/file within the central database.

Various methods can be used to control access to the contents of the central database according to the present invention. Several exemplary techniques are described for establishing a secure central record database according to the present invention.

A feature of this invention is a system that protects from access by unauthorized parties, a record of an individual in a record database, generally and a record in a database accessible via a public network more particularly.

Briefly, this invention contemplates records in a record database (for example, a national medical record database) protected by a digital code generated by a physical characteristic of the person (e.g., an encoded finger print, voice print, signature scan, or retinal scan) attached to each person's protected record in the database in addition to a person's assigned ID code (e.g., Social Security Number). Access via the ID can be selected in accordance with preestablished instructions mandated by the individual. For example, some individuals will be more interested in medical personnel having ready access to their record and can specify instructions consistent with this concern. In addition, some individuals may be concerned about the privacy of certain parts of their medical history, but not others, and can specify instructions consistent with this concern.

In one embodiment of the invention, a protected record cannot be entered or accessed from the national database unless the request is accompanied by the physical characteristic code that matches the physical characteristic code associated with the protected record. Each individual, who participates in the national medical database, can provide via a transducer a physical characteristic sample (e.g., a voiceprint, fingerprint or signature). This sample can be digitally encoded and attached to a person's entire record in the national database. The record can also be stored in the database of the healthcare provider who generates the record and those records can be accessible by that healthcare provider without requiring the physical identifier code if the individual agrees to such access. For the foreseeable future, following the establishment of a national medical database, health care providers can continue to maintain their own databases for the records they generate and, subject to agreement by the individual, can continue to control access to their respective databases. The record can be stored also in the national database, where records can be accessed from authorized terminals by predesignated professionals authorized by the individual using that person's ID. In

contrast, access to protected records can require, in addition to the person's ID, the person's physical characteristic code, which is encoded as part of the request message. To authorize access to or entries into records with a highest level of protection, the system, in one embodiment, can require the physical presence of the individual. Here a transducer associated with the terminal at which the request is made, can transduce and encode the physical characteristic of the person whose protected record is sought and who is authorizing the request.

In one embodiment of the invention, a method for maintaining an individual's record in a record database with access to the record controlled by the individual features the steps of linking a plurality of data input/output terminals to a record database via a network, assigning each individual an ID number code, transducing an identifying characteristic of each individual to a digital identifying characteristic code, storing said ID number code and said digital identifying characteristic code in an ID and identifying code database, calculating an access code by algorithmically combining said ID number code and said digital identifying characteristic code, storing an individual's record in said record database accessible by said access code, querying said record database from one of said plurality of data input/output terminals by transmitting a query that includes sending a query ID number code, and a query digital identifying characteristic code, calculating a query access code by algorithmically combining said query ID number code and said query digital identifying characteristic code, and retrieving a query record from said record database using said query access code, comparing said query ID number code and said query identifying characteristic code transmitted in said querying step with said identifying characteristic code and said ID number code stored in said ID and identifying code database, transmitting said record with said ID number code to said one of said plurality of data input/output terminals in response to said

querying step only if the codes compared in said comparing step match within predetermined limits.

In another embodiment, a method for maintaining an individual's record in a record database with access to the record controlled by the individual features is described including steps of linking a plurality of data input/output terminals to a record database via a network, assigning each individual an ID number code, storing said ID number code in an ID database, transducing an identifying characteristic of each individual to a digital identifying characteristic code, storing said digital identifying characteristic code in an identifying characteristics code database, calculating an access code by algorithmically combining said ID number code and said digital identifying characteristic code, storing said access code in an access code database, storing an individual's record in said record database accessible by said access code, querying said record database from one of said plurality of data input/output terminals by transmitting a query that includes sending a query ID number code, and a query digital identifying characteristic code, calculating a query access code by algorithmically combining said query ID number code and said query digital identifying characteristic code, and retrieving a query record from said record database using said query access code, comparing said query ID number code with said ID number stored in said ID database and comparing said query identifying characteristic code with said identifying characteristic code stored in said identifying characteristic code database, comparing said query access code with said access code stored in said access code database, transmitting said record along with said ID number code to said one of said plurality of data input/output terminals in response to said querying step only if the codes compared in said comparing steps match within predetermined limits.

Another example embodiment features a method for maintaining an individual's record in a record database with access to the record controlled by the individual, including the steps of linking a plurality of data input/output terminals to a record database via a network, assigning each individual an ID number code, transducing an identifying characteristic of each individual to a digital identifying characteristic code, calculating an access code by algorithmically combining said ID number code and said digital identifying characteristic code, storing said access code in an access code database, storing an individual's record in said record database accessible by said access code, querying said record database from one of said plurality of data input/output terminals by transmitting a query that includes, sending a query ID number code, and a query digital identifying characteristic code, calculating a query access code by algorithmically combining said query ID number code and said query digital identifying characteristic code, and retrieving a query record from said record database using said query access code, comparing said query access code with said access code stored in said access code database, transmitting said record along with said ID number code to said one of said plurality of data input/output terminals in response to said querying step only if the codes compared in said comparing step match within predetermined limits.

Further features and advantages of the invention, as well as the structure and operation of various embodiments of the invention, are described in detail below with reference to the accompanying drawings. In the drawings, like reference numbers generally indicate identical, functionally similar, and/or structurally similar elements. The drawing in which an element first appears is indicated by the leftmost digits in the corresponding reference number.

Brief Description of the Drawings

The foregoing and other features and advantages will be better understood from the following detailed description of a preferred embodiment of the invention with reference to the drawings, wherein:

FIG. 1 is a block diagram showing an example workflow providing a patient access to a medical record by using an ID code and a biometric code;

FIG. 2 is a block diagram showing another example workflow with enhanced security features;

FIG. 3 illustrates another workflow method for providing patient medical record access with additional security features; and

FIG. 4 illustrates yet another patient medical record access method having security features.

Detailed Description of a Preferred Embodiment of the Invention

The preferred embodiment of the invention is discussed in detail below. While specific implementations are discussed, it should be understood that this is done for illustration purposes only. A person skilled in the relevant art will recognize that other components and configurations may be used without parting from the spirit and scope of the invention.

FIG. 1 illustratively depicts a block diagram 100 including an example workflow by which a patient 102 can gain access to a record associated with patient 102 at a requesting site 120 according to one embodiment of the present invention. In one embodiment, the block diagram 100 begins with the patient 102 or a person authorized by the patient 102, inputting or being assigned personal identification codes such as, e.g., an ID number code 104 and a

biometric code 106. The personal identification codes 104, 106, can be used to confirm the identity of a person 120 requesting access to a central records database 116. The ID number code 104 and biometric code 106 are inputted into an ID & biometric database 112 as shown by lines 108 and 110, respectively. The ID & biometric database 112 can verify that there is a match between the ID number and biometric inputted into ID number code 104 and biometric code 106 and the records stored in ID & biometric database 112. If both the ID code 104 and biometric code 106 match the records of approved lists of IDs stored in ID & biometric database 112, then access can be granted to a particular record using an ID code 114 which can be used to identify a particular record/file in the central records database 116. The ID code 114 can be used to query records database 116 to obtain the individual record for patient 102. The individual record can be associated with the ID code 114 and can then be transmitted back to the requesting site 120 for use by, e.g., an authorized user such as a doctor. Requesting site 120 could be a doctor's office or a hospital, for example.

FIG. 2 illustratively depicts a block diagram 200 including another example workflow by which patient 102 can gain access to a record associated with patient 102 at a requesting site 120 according to another embodiment of the present invention. The block diagram 200 depicts an another example method which provides enhanced security features. The method of block diagram 200 includes using a special access code 204 to identify (i.e., index) records in a records database 216, instead of ID code 114.

The block diagram 200 begins similarly to diagram 100. As in the technique of FIG. 1, personal identification codes (ID number code 104 and biometric code 106) can be used to confirm the identity of a person such as, e.g., a patient 102, requesting access to a record/file in central records database 216. The ID number code 104 and biometric code 106 can be inputted into ID & biometric database 112 as shown as lines 108 and 110, respectively. If

both the ID number code 104 and biometric code 106 match an approved list in ID & biometric database 112, then a special *access code* 204 can be calculated. The special access code 204 can be calculated by an access code calculator 202 which can receive as input the verified ID number code and biometric code 220. The access code calculator 202 can calculate the special access code 204 by combining the individual's ID number code 104 with one or more biometric codes 106 according to an algorithm, yielding an algorithmic result. One embodiment of the special access code 204 could be a hash digest. In one embodiment of the invention the access code 204 can be calculated by executing an algorithm as shown below in Table 1.

ID Code + Biometric Code(s) + Algorithm = Computed Special Access Code = Access to Protected Record

Table 1.

Special access code 204 can provide access to a separate records database 216, and can be used to identify and grant access to a particular record/file stored in the records database 216.

The technique of the present invention illustrated in FIG. 2 provides a higher level of security than that of FIG. 1. In particular, since the special access code 204 of FIG. 2, used to grant access to and to identify records in the central records database 216, is not known to any individual (i.e., including the individual accessing the information), a higher level of security is maintained. The special access code 204 never leaves the confines of the central record database 216. The central record database 216 itself does not contain any names or other identifying information beyond the special access code 204. If an approved access code 204 is generated, then an individual record associated with the access code 204 can be accessed from the record database 216. Once a record has been accessed via an approved

access code 204, the record can be delivered/transmitted 208 with the access code to an access code match module 210 which can also receive an ID code and access code 206. Access code match module 210 can then associate the individual record with the ID. Access code match module 210 can then transmit the ID and individual record 212 to an individual record with ID storage module 214 which can then be accessed by the authorized requesting individual. Thus the individual record can be sent back to the requesting individual with the original ID code for identification proposes. No other identifiable information, including the special access code 204, need be transmitted back. After the individual record is downloaded and has been used, it can be eliminated or destroyed at the local level to maintain privacy requirements, e.g., using an automatic routine.

FIG. 3 illustratively depicts a block diagram of another method 300 providing an even higher level of security than that shown in FIG. 2. As in the technique of FIG. 2, method 300 uses a central database 316 that contains only the records/files and special access codes 322 needed to grant access to and to identify particular records/files in records database 316.

The method 300 differs from method 200 in several ways.

Method 300 maintains an ID codes database 304 and a biometric database 306. ID number code 104 can be stored 108 in ID database 304. Storing ID number codes 104 in ID database 304 permits a verification comparing an input ID number code 104 to stored ID codes in ID database 304. Similarly, biometric code 106 can be stored 110 in biometric database 306. Storing biometric codes 106 in biometric database 306 permits a verification comparing an input biometric code 106 to stored biometric codes in biometric database 306. Using separate databases 304 and 306 for ID and biometric codes, respectively, increases security since the codes 104 and 106, which together can grant access to the records database 316, are not associated with each other in any single database. Instead, the ID number code

104 and biometric code 106 can be matched to stored ID and biometric codes in ID database 304 and biometric database 306, respectively, to verify that the codes 104 and 106 are valid. Then, as in the previous method, the ID and biometric codes can be inputted as shown with lines 108 and 110 into an access code calculator 302 where the codes 104 and 106 can be combined with an algorithm, such as, e.g., that shown in table 1, to produce a special access code 304. Access code 304 can then be stored in an access code database 320

Before granting access to the records database 316, the special access code 304, just calculated by the access code calculator 302, can be inputted into access code database 320 where the calculated access code 304 can be compared to stored access codes and verified by matching the calculated access code to access codes stored in the access code database 320. This comparison/verification confirms the identity of the requesting individual since only one unique access code can be generated by combining the ID code 104 and biometric code 106. The access code can then be provided to the records database 316 as shown by line 322.

The central record database 316 itself does not contain any names or other identifying information beyond the special access code 304. If an approved access code 322 is generated, then an individual record associated with the access code 322 can be accessed from the record database 316. Once a record has been accessed via an approved access code 322, the record can be delivered/transmitted 308 with the access code 322 to an access code match module 310 which can also receive an ID code and access code 306 from the access code calculator 302. Access code match module 310 can then associate the individual record with the ID. Access code match module 310 can then transmit the ID and individual record 312 to an individual record with ID temporary storage module 314 which can then be accessed by the authorized requesting individual as shown by line 318. Thus the individual record can be sent back to the requesting individual with the original ID code 104 for identification

proposes. No other identifiable information, including the special access code 320, need be transmitted back. After the individual record is downloaded and has been used, it can be eliminated or destroyed at the local level to maintain privacy requirements, e.g., using an automatic routine.

FIG. 4 illustratively depicts a block diagram of another method 40 that increases security of records database 316 even further by eliminating the ID database 304 and biometric database 306, altogether. As in the method 300 described above with reference to FIG. 3, the technique of method 400 combines the ID number code 104 and biometric code 106 with an algorithm to produce a unique special access code 304. If the special access code 304 matches an approved code in access code database 320, then access can be granted to the particular record associated with the valid special access code 322. The technique can continue as described with reference to FIG. 3.

The method 400 of FIG. 4 can provide additional security over method 300 by not maintaining an ID database 304 and biometric database 306 that could possibly be compromised. Method 400 works on the premise that biometric codes 106 are unique throughout the human population and can therefore be used, with the ID code 104, to generate unique access codes 304. Special access codes 30 can be confirmed as valid by the access code database 320 if they correspond to a particular code stored in the access code database 320. As in the above described methods 200 and 300, that also use access codes 204 and 304, the special access codes 204 and 304 are not known outside the central records database 316 or perhaps the access code database 320. Similar steps for transmitting records back to the requesting site can also be followed.

In all the above-described methods, a protected record cannot be entered or accessed from the central database 216 and 316 unless a valid ID code 104 and one or more valid

biometric physical characteristic codes 106 accompany the request. These biometric codes 106 can be time-stamped in order to protect against fraud and to insure only current requests are approved (to prevent biometric re-use from illegally intercepted transmissions).

Each individual, who participates in the central database 216 and 316, provides, e.g., via a transducer, one or more physical biometric characteristic samples such as, e.g., a voice sample, fingerprint, or a signature. These samples can be digitally encoded, can be attached, can possibly be placed in an encrypted form, and can be associated with a person's entire record in the central database. Alternatively, as described in methods 200, 300 and 400, special access codes 204 and 304 can be generated/calculated when a record is initially created or modified via an algorithm that combines the biometric samples 106 and assigned ID code 104. Although unknown to the individual, these special access codes 204 and 304 can be attached to the record and in one embodiment, can only be generated via the correct ID code 104 and biometric code 106.

If an individual loses or forgets the individual's ID code 104 (i.e., ID codes 104 can be stored on magnetic and smart card systems), the ID code 104 can be recreated by a system that in one embodiment, accepts two or more biometric codes, or other enhanced identity verification, to provide a highly accurate procedure to confirm an individual's identity.

Access to records can be restricted in accordance with pre-established instructions mandated by the individual. For example, some individuals can be more interested in medical personnel having ready access to their record and can specify instructions consistent with this desire. In addition, some individuals may be concerned about the privacy of certain parts of their medical history, but not other parts, and can therefore, e.g., specify instructions consistent with these concerns. People that have approval or authorization from an individual can be provided, in one embodiment, the ability to access that individual's record via that

individual's ID and their own biometric identifier code or codes. Approved people can produce a special access code 204 and 304, if required, that could grant them access to a particular individual's records. In one embodiment, an authorized person can, e.g., by using the individual's ID and their own biometric characteristic codes, be granted access to a particular individual's records. The use of biometric codes can also provide an added level of security by, e.g., allowing precise tracking of who has accessed an individual's records over a period of time.

Separately, access to the central records database 216 and 316 can be rendered harmless to privacy concerns, because names and other common forms of information used to identify individuals are absent from the medical records database 316. This feature provides an added benefit to researchers, such as, e.g., epidemiological and clinical medical researchers in a medical records database, who can be given access to the central database 216 and 316 without risk of identifying particular individuals since any identification data is encoded, encrypted or not even in a readily accessible form.

To authorize access to records with a highest level of protection, the present invention can require the physical presence of the individual to provide biometric code 106 input. In such an embodiment, a transducer associated with the entry terminal at which the request is made, can transduce and encode the physical biometric characteristics 106 of the person whose protected record is sought and who is authorizing the request. As described before, the biometric code or codes 106 can also be time-stamped for additional security. Additionally, the records themselves in the central records database 216 and 316 can be encrypted.

In one embodiment, following establishment of central record databases 216 and 316, some organizations can be authorized to continue to maintain their own separate databases for records that they generate, and, subject to agreement by the individual, can continue to control

access to their respective databases. In one embodiment, records that are in a central database 216 and 316 can also, subject to agreement by the individual, be stored in the database of the organization that generates the record such as, e.g., a healthcare provider, or a financial organization. The separately stored records can be accessible by the organization without requiring the biometric identifier code 106, i.e., if the individual agrees to such access.

While the invention has been described in terms of a preferred embodiment, those skilled in the art will recognize that the invention can be practiced with modification within the spirit and scope of the appended claims. Particularly, while the invention has been described in connection with protecting an individual's records in medical record database, it will be appreciated that the invention is applicable to the protection of an individual's records in any database.

Claims

Having thus described my invention, what I claim as new and desire to secure by Letters Patent is as follows:

1. A method for maintaining an individual's record in a record database with access to the record controlled by the individual, comprising the steps of:

linking a plurality of data input/output terminals to a record database via a network;

assigning each individual an ID number code;

transducing an identifying characteristic of each individual to a digital identifying characteristic code;

storing said ID number code and said digital identifying characteristic code in an ID and identifying code database;

storing an individual's record in said record database accessible by an ID code;

querying said record database from one of said plurality of data input/output terminals by transmitting a query that includes said ID number code, and said identifying characteristic code;

comparing said ID number code and said identifying characteristic code transmitted in said querying step with said identifying characteristic code and said ID number code stored in said ID and identifying code database;

transmitting said record to said one of said plurality of data input/output terminals in response to said querying step only if the codes compared in said comparing step match within predetermined limits.

2. The method according to claim 1 wherein said record database is maintained in encrypted form.

3. The method according to claim 1 wherein said record database is a national medical record database.

4. The method according to claim 1 wherein said record database is a national record database established by a government agency or mandated by a government or by a government agency.

5. The method according to claim 1 wherein said record database is a medical record database.

6. The method according to claim 1 wherein said record database is a national medical record database established by a government agency or mandated by a government or by a government agency.

7. The method according to claim 1 including the further step of entering and/or updating a record in response to said addressing step only if the codes compared in said step match within a predetermined time period.

8. The method according to claim 1 wherein said plurality of data inputs/output terminals are linked to said record database by a wide area, publicly accessible network.

9. The method according to claim 8 wherein said network utilizes the Internet and/or worldwide web.

10. The method according to claim 1 wherein said transducing step is carried out contemporaneously with said addressing step.

11. The method according to claim 7 wherein said transducing step is carried out contemporaneously with said addressing step.

12. The method according to claim 8 wherein said transducing step is carried out contemporaneously with said addressing step.

13. The method according to claim 9 wherein said transducing step is carried out contemporaneously with said addressing step.

14. The method according to claim 2 wherein said record database is a national medical record database.

15. The method according to claim 2 wherein said record database is a national record database established by a government agency or mandated by a government or by a government agency.

16. The method according to claim 2 wherein said record database is a medical record database.

17. The method according to claim 2 wherein said record database is a national medical record database established by a government agency or mandated by a government or by a government agency.

18. The method according to claim 2 including the further step of entering and/or updating a record in response to said addressing step only if the codes compared in said step match within a predetermined time period.

19. The method according to claim 2 wherein said plurality of data inputs/output terminals are linked to said record database by a wide area, publicly accessible network.

20. The method according to claim 19 wherein said network utilizes the Internet and/or the worldwide web.

21. The method according to claim 2 wherein said transducing step is carried out contemporaneously with said addressing step.

22. The method according to claim 18 wherein said transducing step is carried out contemporaneously with said addressing step.

23. The method according to claim 19 wherein said transducing step is carried out contemporaneously with said addressing step.

24. The method according to claim 20 wherein said transducing step is carried out contemporaneously with said addressing step.

25. A method for maintaining an individual's record in a record database with access to the record controlled by the individual, comprising the steps of:

linking a plurality of data input/output terminals to a record database via a network;

assigning each individual an ID number code;

transducing an identifying characteristic of each individual to a digital identifying characteristic code;

storing said ID number code and said digital identifying characteristic code in an ID and identifying code database;

calculating an access code by algorithmically combining said ID number code and said digital identifying characteristic code;

storing an individual's record in said record database accessible by said access code;

querying said record database from one of said plurality of data input/output terminals by transmitting a query that includes

sending a query ID number code, and a query digital identifying characteristic code,

calculating a query access code by algorithmically combining said query ID number code and said query digital identifying characteristic code, and

retrieving a query record from said record database using said query access code;

comparing said query ID number code and said query identifying characteristic code transmitted in said querying step with said identifying characteristic code and said ID number code stored in said ID and identifying code database;

transmitting said record with said ID number code to said one of said plurality of data input/output terminals in response to said querying step only if the codes compared in said comparing step match within predetermined limits.

26. A method for maintaining an individual's record in a record database with access to the record controlled by the individual, comprising the steps of:

linking a plurality of data input/output terminals to a record database via a network;

assigning each individual an ID number code;

storing said ID number code in an ID database;

transducing an identifying characteristic of each individual to a digital identifying characteristic code;

storing said digital identifying characteristic code in an identifying characteristics code database;

calculating an access code by algorithmically combining said ID number code and said digital identifying characteristic code;

storing said access code in an access code database;

storing an individual's record in said record database accessible by said access code;

querying said record database from one of said plurality of data input/output terminals by transmitting a query that includes

sending a query ID number code, and a query digital identifying characteristic code,

calculating a query access code by algorithmically combining said query ID number code and said query digital identifying characteristic code, and

retrieving a query record from said record database using said query access code;

comparing said query ID number code with said ID number stored in said ID database and comparing said query identifying characteristic code with said identifying characteristic code stored in said identifying characteristic code database;

comparing said query access code with said access code stored in said access code database;

transmitting said record along with said ID number code to said one of said plurality of data input/output terminals in response to said querying step only if the codes compared in said comparing steps match within predetermined limits.

27. A method for maintaining an individual's record in a record database with access to the record controlled by the individual, comprising the steps of:

linking a plurality of data input/output terminals to a record database via a network;

assigning each individual an ID number code;

transducing an identifying characteristic of each individual to a digital identifying characteristic code;

calculating an access code by algorithmically combining said ID number code and said digital identifying characteristic code;

storing said access code in an access code database;

storing an individual's record in said record database accessible by said access code;

querying said record database from one of said plurality of data input/output terminals by transmitting a query that includes

sending a query ID number code, and a query digital identifying characteristic code,

calculating a query access code by algorithmically combining said query ID number code and said query digital identifying characteristic code, and

retrieving a query record from said record database using said query access code;

comparing said query access code with said access code stored in said access code database;

transmitting said record along with said ID number code to said one of said plurality of data input/output terminals in response to said querying step only if the codes compared in said comparing step match within predetermined limits.

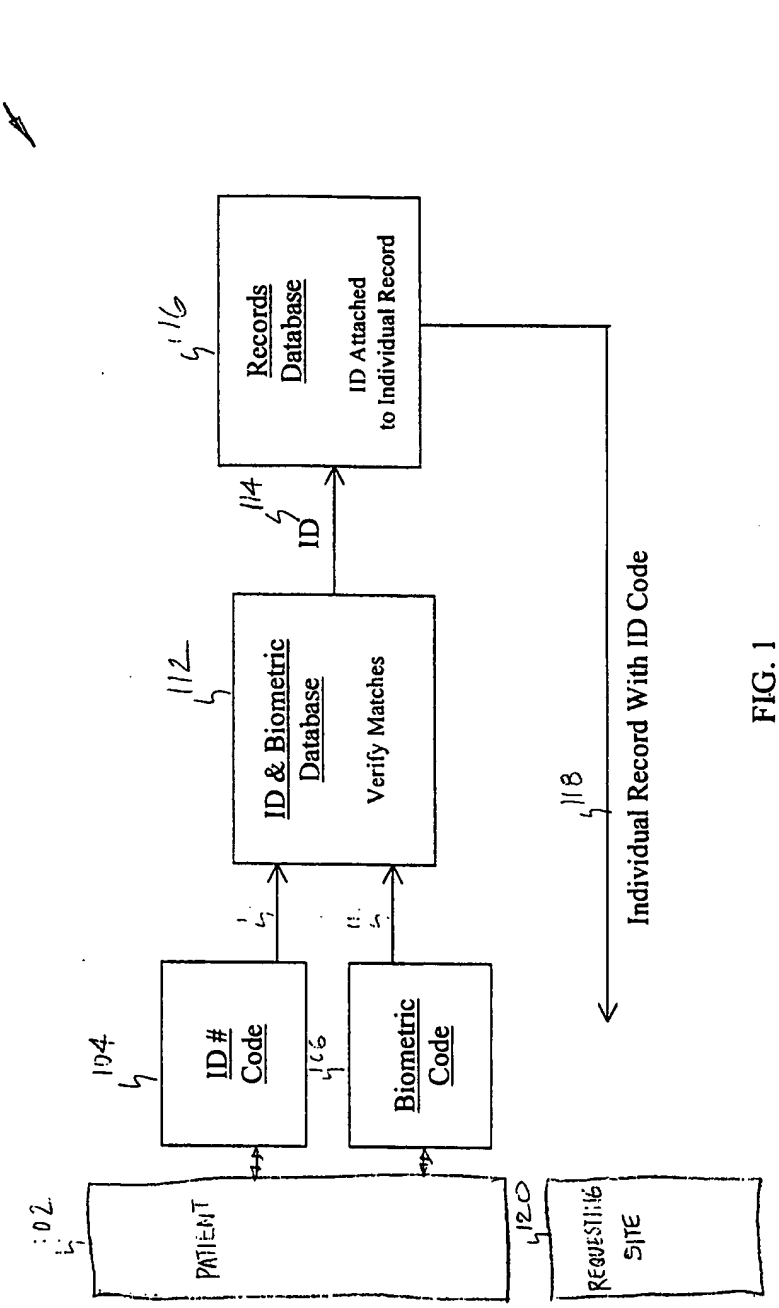

100
Records Database
ID Attached to Individual Record
116
114
ID
ID & Biometric Database
Verify Matches
112
Individual Record With ID Code
118
ID # Code
104
Biometric Code
106
PATIENT
102
REQUESTING SITE
120

FIG. 1

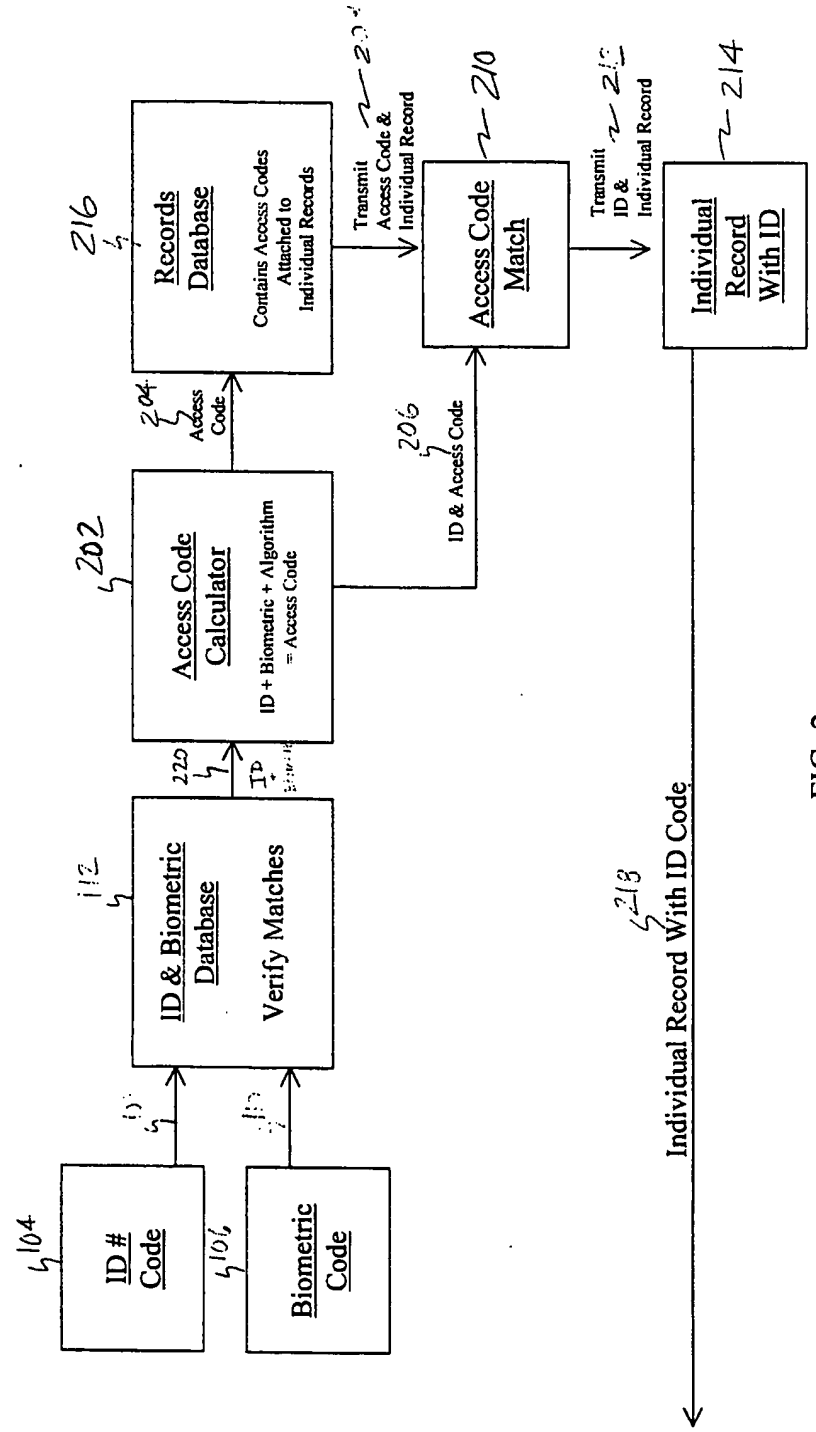

200
ID # Code
104
Biometric Code
106
ID & Biometric Database
112
Verify Matches
220
ID + Biometric + Algorithm = Access Code
Access Code Calculator
202
Access Code
204
ID & Access Code
206
Records Database
216
Contains Access Codes Attached to Individual Records
Transmit Access Code & Individual Record
Access Code Match
210
Transmit ID & Individual Record
Individual Record With ID
214
Individual Record With ID Code
218

FIG. 2

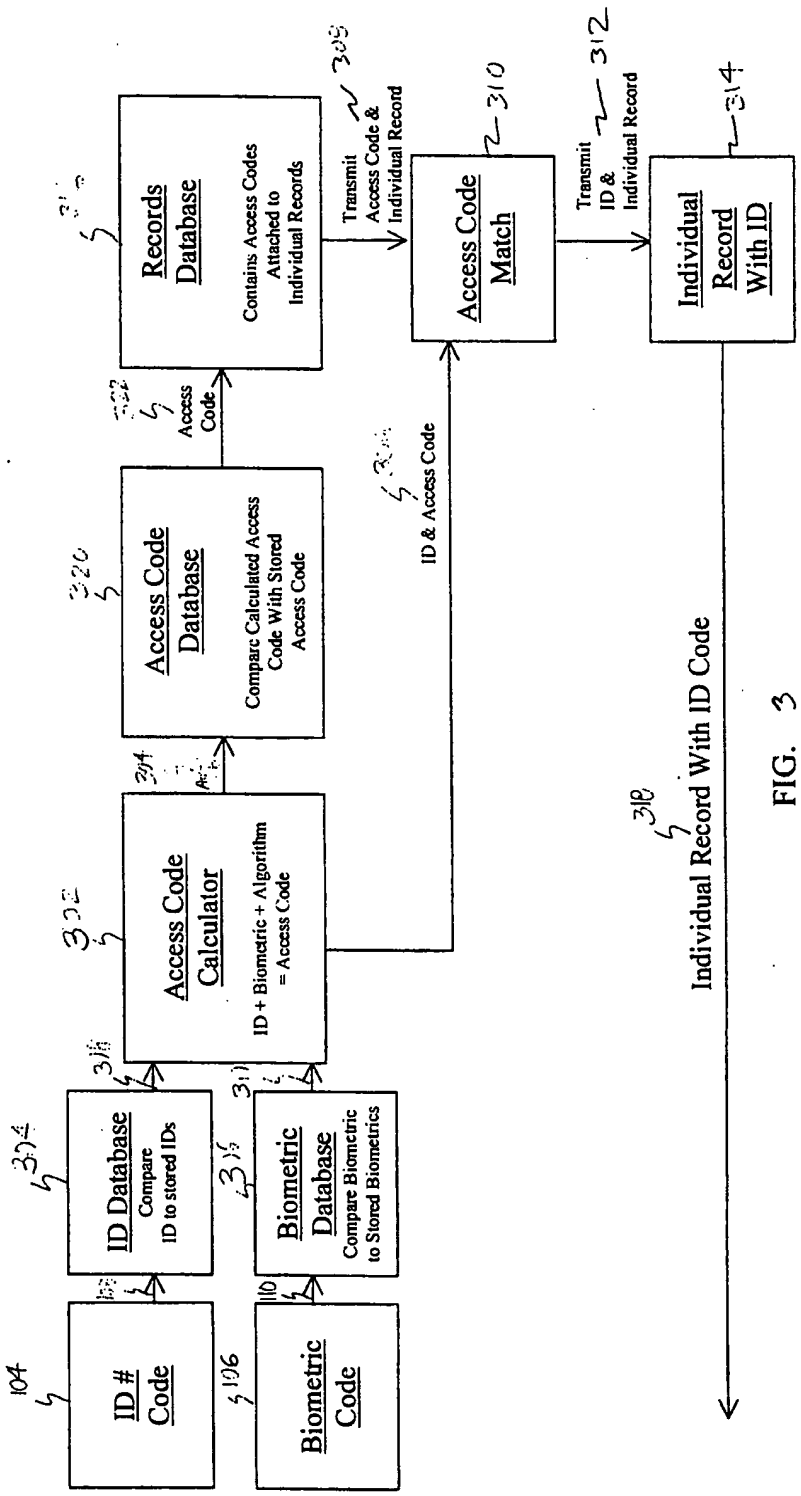

300
ID # Code
104
Biometric Code
106
ID Database
Compare ID to stored IDs
324
Biometric Database
Compare Biometric to Stored Biometrics
316
Access Code Calculator
ID + Biometric + Algorithm = Access Code
322
Access Code Database
Compare Calculated Access Code With Stored Access Code
320
Records Database
Contains Access Codes Attached to Individual Records
Access Code
Transmit Access Code & Individual Record
305
ID & Access Code
Access Code Match
310
Transmit ID & Individual Record
312
Individual Record With ID
314
Individual Record With ID Code
318

FIG. 3

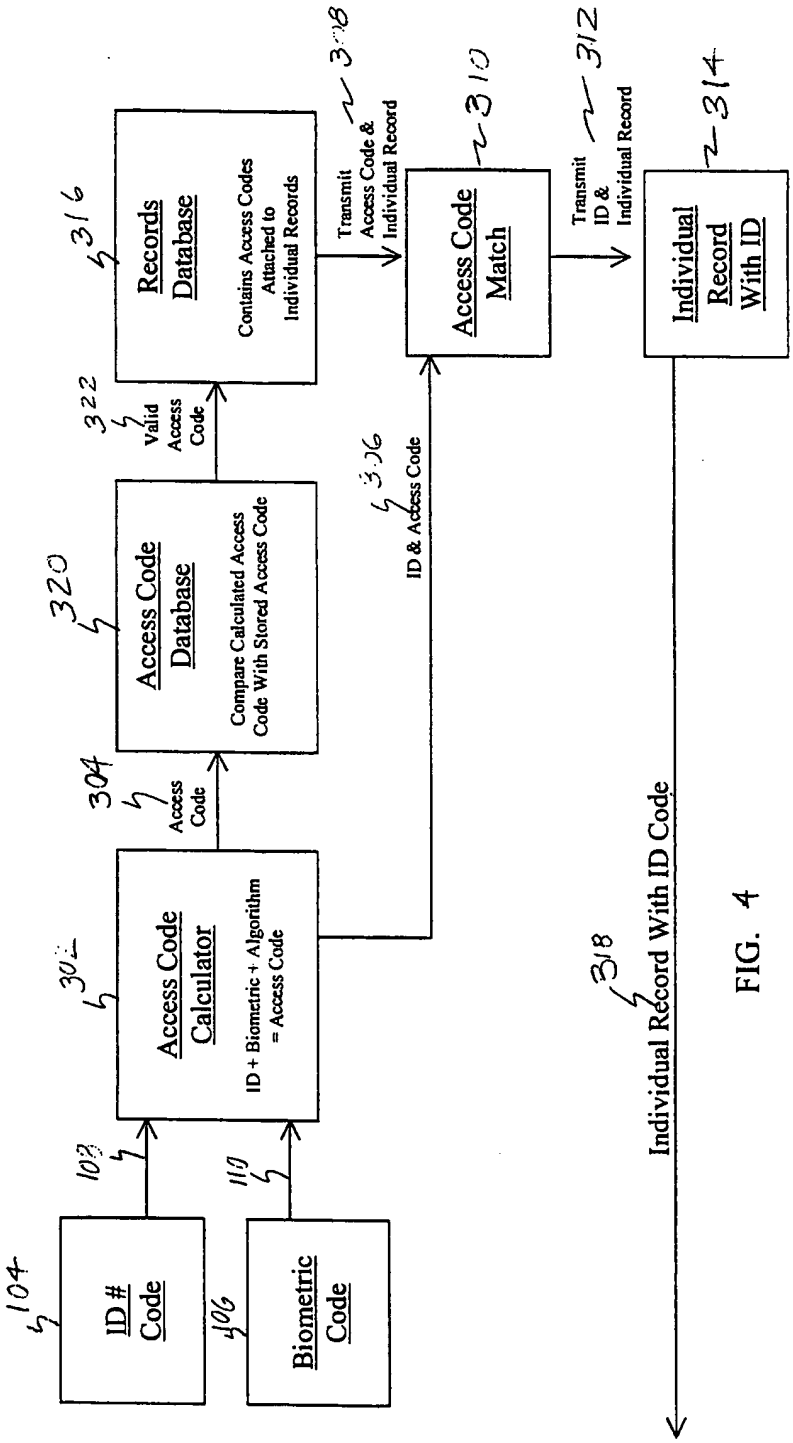

400
ID # Code
104
Biometric Code
106
102
110
Access Code Calculator
ID + Biometric + Algorithm = Access Code
302
304
Access Code
Access Code Database
Compare Calculated Access Code With Stored Access Code
320
322
Valid Access Code
Records Database
Contains Access Codes Attached to Individual Records
316
308
Transmit Access Code & Individual Record
306
ID & Access Code
Access Code Match
310
312
Transmit ID & Individual Record
Individual Record With ID
314
318
Individual Record With ID Code

FIG. 4

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US99/26090

A. CLASSIFICATION OF SUBJECT MATTER

IPC(6) :G06F 17/30
US CL :707/1, 3; 705/2, 3, 4.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 707/1, 3; 705/2, 3, 4.

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

WEST, IBM TECHNICAL
search terms: records database, access, query, id code, encryption

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5,644,778 A (BURKS et al) 01 July 1997, col. 1, lines 44-67, col. 3, lines 1-25, col. 5, lines 41-65, col. 6, lines 24-67, col. 7, lines 1-9, and col. 9, lines 52-67.	1-27
Y	US 5,579,393 A (CONNER et al) 26 November 1996, col. 5, lines 16-42, col. 6, lines 10-30, col. 7, lines 7-37, col. 11, lines 1-38 and lines 59-67, col. 12, lines 1-18 and lines 66-67, col. 13, lines 1-18, col. 20, lines 50-65, col. 21, lines 26-67, and col. 22, lines 1-16.	1-27

[X] Further documents are listed in the continuation of Box C. [ ] See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E"	earlier document published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search	Date of mailing of the international search report
10 FEBRUARY 2000	02 MAR 2000

Name and mailing address of the ISA/US	Authorized officer
Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231	Hosain Alam FOR Virginia Logan
Facsimile No. (703) 305-3230	Telephone No. (703) 308-6662

Form PCT/ISA/210 (second sheet)(July 1992)*

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US99/26090

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5,659,741 A (EBERHARDT) 19 August 1997, col. 3, lines 47-67, col. 4, lines 14-22, col. 8, lines 45-52 and lines 62-67, col. 9, lines 1-49, col. 10, lines 45-67, col. lines 1-35, col. lines 22-30 and lines 54-57, and col. 16, lines 30-38.	1-27
Y	US 5,193,855 A (SHAMOS) 16 March 1993, col. 2, lines 10-38, col. 3, lines 32-68, col. 4, lines 1-11, col. 5, lines 7-47, and col. 9, lines 31-51.	1-27
Y	US 5,664,109 A (JOHNSON et al) 02 September 1997, col. 1, lines 51-67, col. 2, lines 1-67, col. 3, lines 1-10 and lines 28-35, col. 4, lines 41-67, col. 5, lines 1-12 and lines 55-67, col. 6, lines 1-7, col. 9, lines 38-65, col. 11, lines 43-67, col. 12, lines 1-31, col. 14, lines 4-67, and col. 15, lines 1-5 and lines 20-38.	1-27